[illegible] Regulation [illegible]

Military Intelligence

U.S. Army Counterintelligence Activities

[illegible]
Department of the [illegible]
Washington, DC
[illegible]

SUMMARY of CHANGE

AR 381-20
U.S. Army Counterintelligence Activities

This regulation--

- Contains major revisions concerning the definition, conduct of, and jurisdiction over counterintelligence investigation, production, collection, and liaison per DOD Directive 5240.2 (chap 1 through 9).

- Updates Army intelligence organization and responsibilities (chap 1).

- Adds new directives on counterintelligence support to terrorism counteraction (chap 3).

Headquarters
Department of the Army
Washington, DC
26 September 1986

*Army Regulation 381-20

Effective 27 October 1986

Military Intelligence

U.S. Army Counterintelligence Activities

This UPDATE printing publishes a revision which is effective 27 October 1986. Because the structure of the entire revised text has been reorganized, no attempt has been made to highlight changes from the earlier regulation dated 10 September 1975.

By Order of the Secretary of the Army.

JOHN A. WICKHAM, JR.
General, United States Army
Chief of Staff

Official:

R. L. DILWORTH
Brigadier General, United States Army
The Adjutant General

Summary. This regulation establishes the authority and responsibility for the conduct of U.S. Army counterintelligence (CI) activities. It includes guidance on the definition, conduct of, and jurisdiction over CI investigation, production, collection, and liaison. It implements DOD Directive 5240.2.

Applicability. This regulation—

a. Applies to all Army intelligence components, other military personnel and civilian employees of the Department of the Army when they engage in intelligence activities, and members of the Army National Guard and U.S. Army Reserve when they perform Federal duties or engage in activities directly related to a Federal duty or mission.

b. Does not apply to activities covered under Presidential Directive/National Security Council–9.

Impact on the New Manning System. This regulation does not contain information that affects the New Manning System.

Internal control system. This regulation is not subject to the requirements of AR 11–2. It does not contain internal control provisions.

Supplementation. Supplementation of this regulation and establishment of forms other than DA forms are prohibited without prior approval from HQDA (DAMI–CIC), WASH DC 20310–1054.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested improvements. The proponent agency of this regulation is the Office of the Assistant Chief of Staff for Intelligence. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI–CIC), WASH DC 20310–1054.

Distribution. Distribution of this issue has been made in accordance with DA Form 12–9A–R requirements for 381 series publications. The number of copies distributed to a given subscriber is the number of copies requested in Block 335 of the subscriber's DA Form 12–9A–R. AR 381–20 distribution is A for Active Army, ARNG, and USAR.

Contents (Listed by paragraph number)

b. All investigations will be conducted in accordance with this regulation.

c. Investigations will be coordinated with other intelligence and law enforcement agencies as necessary and appropriate. Departmental CI investigative jurisdiction is defined in appendix C.

d. Investigations will continue until allegations are resolved, adequate intelligence information is provided to responsible officials, or the control office determines that the investigation may be closed, suspended, or terminated.

e. Investigations will be conducted only by CI personnel (who have been issued badges and credentials and are school-trained in specialty skill identifier (SSI) 36A or 36B, or military occupational specialty (MOS) 971A, 972A, 97B, or 97C) or by Army civilian employees, assigned to operational duties in CI units, and appropriately trained and issued badges and credentials.

2–2. Investigations under Army CI jurisdiction

a. CI investigative jurisdiction is derived from national, DOD, and Army policy that defines the types of incidents and status of personnel who are subject to investigation by Army CI components. All investigative activity directed against U.S. persons, or employing certain intrusive investigative techniques, must comply with AR 381–10.

b. Army CI jurisdiction includes the following activities:

(1) Known or suspected acts of espionage.

(2) CI aspects of known or suspected foreign-directed sabotage.

(3) Subversive activity by Army personnel.

(4) Known or suspected acts of treason by Army personnel.

(5) Known or suspected acts of sedition by Army personnel.

(6) CI aspects of terrorist activities.

(7) CI aspects of assassination or attempted assassination of Army personnel by terrorists or by agents of a foreign power.

(8) Defection of Army military or civilian personnel, to include investigation of the circumstances surrounding the defection and debriefing of the individual upon return to U.S. control.

(9) Detention of Army military or civilian personnel by a government or hostile force with interests inimical to those of the United States, to include debriefing the individual upon return to U.S. control.

(10) Investigation and debriefing of knowledgeable personnel absent without leave (KAWOL).

(11) CI aspects of security violations and compromises to include acts or suspected acts of deliberate compromise or willful disclosure of classified information or material, and COMSEC insecurities.

(12) Impersonation of Army military intelligence personnel or the unlawful possession or use of military intelligence identification.

(13) Violations by Army personnel of the Intelligence Identities Protection Act (50 USC 421).

c. Within the United States, Army CI has investigative jurisdiction over the following persons:

(1) U.S. Army personnel on active duty.

(2) Retired Army personnel.

(3) Active and Inactive members of the U.S. Army Reserve (USAR) and Army National Guard (ARNG), when the act under investigation took place while the individual was on active duty.

d. If the FBI waives jurisdiction over Army civilian employees, Army CI may take investigative actions necessary to—

(1) Establish the basis for administrative action by DA against these employees.

(2) Protect the security of Army personnel, information, functions, activities, and installations.

e. Outside the United States, Army CI has investigative jurisdiction over the following persons (unless responsibility is otherwise assigned by agreement with host government, U.S. law, or Executive directive):

(1) Army personnel on active duty.

(2) Family members of active duty Army personnel.

(3) Army civilian employees and their family members.

(4) Army contractors, their employees, and family members.

(5) Retired Army personnel, active and inactive USAR personnel, ARNG members, and other U.S. persons, subject to coordination with the FBI, CIA, and host government agencies.

(6) Foreign nationals who are applicants for, or are employed in, positions requiring access to U.S. classified information.

(7) Other foreign nations, subject to coordination with the CIA and agreements with other DOD intelligence components and host nation governments.

f. In addition, Army CI may take investigative actions necessary to—

(1) Establish the basis for administrative action by DA.

(2) Protect the security of Army personnel, information, functions, activities, and installations.

g. Army CI jurisdiction includes both the investigation of known or suspected acts against the Army (incident investigations), as well as the investigation of personnel believed to be involved in activities listed in *b* above (personal subject investigations). These investigations are subject to DOD agreement with the Department of Justice (App C) and applicable Status of Forces agreements.

h. In those instances where primary jurisdiction rests with another Federal or State agency, Army investigation will normally take the form of coordinating with the primary agency, providing assistance as required, and acquiring copies of reports and determinations collectable under AR 381–10.

2–3. Control offices

The DA Central Control Office established by the CG, INSCOM and the sub-control offices established by CINCUSAREUR; CG, Eighth U.S. Army; and the commanders of the 470th, 500th, and 902nd MI Groups, have the authority to initiate, direct, and terminate CI investigations in accordance with this regulation. Specifically, the sub-control offices will—

a. Initiate investigations based on information received from field elements, liaison channels, or other sources.

b. Within 5 working days after initiation, provide the following information to the DA Central Control Office, with follow up reports as required:

(1) Source and substance of information leading to the initiation of the investigation.

(2) Subject of the investigation.

(3) Summary of investigative activities being undertaken.

(4) Other Army or intelligence community elements involved or tasked in the investigation.

c. Disseminate appropriate tasking and monitor the conduct of investigations within their area of responsibility.

d. Provide investigative guidance as required.

e. Review and coordinate requests for use of investigative techniques requiring approval. (See AR 195–6 and AR 381–10.)

f. Coordinate investigations with other control offices as required.

g. Complete and terminate investigations and transmit investigative reports and summaries to the DA Central Control Office (para 2–4) and to HQDA or the MACOM commander when required.

2–4. DA Central Control Office

The DA Central Control Office acts for Headquarters, Department of the Army (HQDA) in the overall control and coordination of all Army CI investigations. Specifically, the DA Central Control Office will—

a. Exercise direct case control over category I counter-espionage investigations (AR 381–12–1). The DA Central Control Office will ensure that category I cases impacting on USAREUR and Eighth U.S. Army are fully coordinated with the appropriate sub-control office. The DA Central Control Office will open and close such cases, may impart operational or investigative guidance, and will be an action addressee on all relevant reporting and correspondence. USAREUR, Eighth U.S. Army, and 470th, 500th, and 902nd MI Group sub-control offices will continue to exercise all other sub-control office functions stated in paragraph 2–3.

b. Monitor all CI investigations conducted within the Army, and provide guidance and direction to control offices as required.

c. Conduct national liaison with the FBI, CIA, and other Federal departments and agencies as required.

d. Within 10 working days of receipt, review and forward the initiation report (para

HQDA (DAMI-CIC), WASH DC 20310–1054.

e. Prepare followup reports on investigations in sufficient detail for the ACSI to keep senior DA and DOD officials advised of information of possible national interest. This follow up will include notice of termination of the investigation and final action taken by Army CI.

f. Ensure that investigative techniques requiring prior approval have such approval before use, and assist control offices in securing approval.

g. Ensure that information concerning possible loss or compromise of COMSEC information and any occurrence that may jeopardize the security of COMSEC material is provided to appropriate COMSEC organizations in accordance with TB 380–41, chapter 10.

h. Present a semiannual briefing to the ACSI on all investigations of DA interest, including the topics below. (This briefing may be combined with briefings required by AR 381–47.)

(1) Summary of significant activities.

(2) Significant developments.

(3) Statistics by area, type, status, and trends.

i. Receive, process, and transmit investigative and operational records to the Intelligence Records Repository in accordance with AR 381–45.

2–5. Reporting of CI Information

a. All Army commanders who become aware of information that is or may be of CI interest will promptly report this information to the supporting INSCOM CI element. In the absence of a nearby INSCOM element, the information will be reported to the CI element of the nearest tactical MI unit. Units belonging to the Supreme Headquarters Allied Powers Europe and Allied Command Europe who become aware of information of CI interest will report this information immediately to the nearest office of the 650th MI Group.

b. In view of the increased application of analysis and production to CI support to OPSEC, terrorism counteraction, and other security requirements, CI elements will ensure the rapid exchange of information outside immediate command channels. CI elements that obtain raw CI information relating to OPSEC, terrorism, and other security matters, will forward the information to analysis and production centers using the Intelligence Information Report (IIR) format. (This report is exempt from reporting requirement by AR 335–11, para 5–2*e*(2).)

2–6. Shared Investigative Jurisdiction

Intelligence and related crimes of actual or alleged acts of espionage, treason, sabotage, and sedition may present situations where MI and CID have concurrent investigative jurisdiction. The primary responsibility of MI is to investigate such incidents for intelligence and security-related purposes; CID shares the responsibility to investigate the incident for the purpose of reporting crime within Army investigative jurisdiction. The lead agency concept will be employed, based on coordination with the appropriate CID component, to determine which agency will undertake primary investigative responsibility. Generally, MI will take the investigative lead to first exhaust all intelligence/security dimensions of incidents of espionage, treason, and sedition before investigation for possible criminal prosecution is initiated. Generally, CID will assume the investigative lead for actual or suspected incidents of sabotage. Should jurisdictional disputes arise, or should security considerations preclude local coordination, the matter should be referred to HQDA (DAMI-CI), WASH DC 20310–1054, for resolution at HQDA level.

Chapter 3
Counterintelligence Support to Terrorism Counteraction

3–1. Scope

This chapter prescribes policies and procedures and assigns responsibilities for CI support to terrorism counteraction.

3–2. Responsibilities

a. The ACSI will provide guidance and develop policies, plans, and procedures for the collection, analysis, and reporting of information on terrorist activities.

b. The CG, INSCOM will—

(1) Conduct foreign intelligence (FI) and CI activities to collect and disseminate information on all aspects of terrorism and terrorist threats against the Army and DOD. These activities will be conducted in accordance with AR 381–10, AR 381–15, AR 381–20, AR 381–47 and AR 381–100.

(2) Operate a 24–hour operations center to receive and disseminate worldwide terrorism threat information to and from applicable INSCOM staff elements, subordinate commands, and national agencies. On receipt of terrorism-related traffic from INSCOM reporting channels, this operations center will ensure dissemination to all affected units and appropriate DA, DOD, and national agencies.

(3) Provide Army commanders with information on terrorist threats concerning their personnel, facilities, and operations.

(4) Investigate terrorist incidents for intelligence aspects together with the FBI or host nation authorities.

(5) Include terrorist threat information in subversion and espionage directed against U.S. Army (SAEDA) briefings per AR 381–12.

(6) Serve as the Army's liaison representative to Federal, State, and local agencies, and host country national, state, and local-level agencies, to exchange terrorist information.

c. The CG, USAIA will—

(1) Analyze information on all aspects of terrorism and the threat it poses to U.S. Army personnel, facilities, and activities.

(2) [illegible] formation on terrorist threats concerning their personnel, facilities, and activities.

(3) Provide terrorism analysis and threat assessments in response to Army Staff requirements.

(4) Serve as the Army's analytic representative for terrorism intelligence.

d. Intelligence staffs at all levels will—

(1) Promptly report all actual or suspected terrorist incidents, activities, and early warnings of terrorist attack to their chain of command, supported and supporting activities, local INSCOM office, and the USAITAC.

(2) Initiate and maintain liaison with, as a minimum, the provost marshal's office (PMO), local CID and INSCOM elements, security officers and managers, host nation intelligence and security agencies, and other organizations, elements, and individuals as required for the efficient conduct of the mission.

(3) Develop and present terrorism awareness training briefings to all personnel within their command.

e. Law enforcement staffs at all levels will—

(1) Promptly report all actual or suspected terrorist incidents and activities to their chain-of-command, other activities potentially affected, and local INSCOM CI elements.

(2) Initiate and maintain liaison with local INSCOM CI elements.

f. Installation security officers/managers will—

(1) Promptly report all actual or suspected terrorist incident(s) and activities to their chain-of-command, other activities potentially affected, and local INSCOM CI and CID offices. In addition, they will conduct regular liaison with their local PMO, INSCOM CI, and CID representatives, and local intelligence staffs.

(2) Ensure that terrorism threat awareness training and briefings are presented to their personnel.

3–3. Reporting of terrorism information

a. Commanders will report acts of terrorism and other major disruptions on installations in accordance with AR 190–52, with immediate telephonic notification to the Army Operations Center (AOC AUTOVON 851–1800, or commercial (202) 697–0218, and to the MACOM emergency operations center. This will be followed by additional electrical messages, detailing substantive facts as they become available, to HQDA WASH DC//DAPE-HRE//. Additional message information addressees will include HQDA WASH DC//DAMI-DAMO//, CDR USAITAC AHS VA//AIAIT-KT//, and CDR USACIDC WASH DC//CIOP-IS//.

b. The initial report will provide a narrative description of the event to the AOC

tion of occurrence, number of persons involved (hostages and abductors), specifics of demands, and current status.

Chapter 4
Counterintelligence and Security Support Activities

4–1. Scope

This chapter prescribes policies and procedures and assigns responsibilities for CI and security support to U.S. Army OPSEC programs.

4–2. Policy

a. OPSEC is concerned with the maintenance of security and achievement of surprise in U.S. military operations and activities through the protection of capabilities and intentions from hostile intelligence exploitation. Its ultimate objective is to prevent an enemy from obtaining sufficient advance information to predict, and thus be able to degrade, friendly operations or capabilities.

b. OPSEC is a command responsibility. Command OPSEC programs are established and conducted in accordance with AR 530–1. To carry out assigned OPSEC responsibilities, the commander requires support from several sources, to include the military intelligence community. MI OPSEC support is provided by MI components at both echelons above corps (EAC), and echelons corps and below (ECB).

c. CI and security support to OPSEC is only one part of the Army OPSEC program, although it is a major contributing factor. This support takes three basic forms:

(1) Information acquired through internal command security programs to include information security (AR 380–5) and personnel security (AR 604–5).

(2) Information acquired through on-going Army CI programs (AR 381–12, AR 381–47, and this regulation).

(3) Programs specifically developed and tailored to provide security support to the commander as described herein.

d. Because the hostile intelligence threat arrayed against U.S. forces and agencies is multidisciplined, the countering of that threat must also be multidisciplined. Counterintelligence support recognizes the need for a requirement that counters hostile human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT) collection and provides an analytic capability to bring threat, friendly forces vulnerabilities, and existing security programs together. CI and security support to OPSEC satisfies this requirement and is applicable to all echelons from battalion to department level.

e. Recommendations by supporting MI elements for improvements to OPSEC are not directive in nature, unless provided for in other regulations or endorsed as such by the supported commander. The priority and resource allocation decisions that must be considered in implementing OPSEC improvements remain a command responsibility. OPSEC evaluations made by supporting MI elements should be considered, though, by the MACOMs and HQDA in evaluating the overall effectiveness of the MACOM and DA OPSEC programs.

4–3. CI and security support to OPSEC

a. The level of CI and security support to OPSEC will be tailored to the sensitivity of the supported organization and its vulnerability to hostile intelligence collection and terrorist attack.

b. Supporting MI elements will routinely consider the following in determining the degree of CI and security support required:

(1) All aspects of the supported organization's activities. This includes contracts and contractor facilities, weapons systems (special/new), communications systems, and interfaces with other military departments, DOD, other Federal agencies, and foreign governments as appropriate.

(2) The total threat from hostile intelligence collection and terrorist attack capabilities.

(3) Specific identification of vulnerabilities to hostile intelligence collection and terrorist attack.

(4) The regulatory requirements, such as the requirement for cryptofacility inspections.

(5) Recommendations of countermeasures for the supported organization's activities.

4–4. Responsibilities

a. Deputy Chief of Staff for Operations and Plans (DCSOPS). See AR 530–1 for responsibilities of the DCSOPS as they apply to this chapter.

b. Assistant Chief of Staff for Intelligence. The ACSI will—

(1) Formulate policy for intelligence and security support to OPSEC.

(2) Provide HQDA staff supervision over Army intelligence and security support to OPSEC programs.

c. CG, INSCOM. Within assigned resources, the CG, INSCOM will—

(1) Provide intelligence and security support to the OPSEC programs of the Army Staff, all elements at EAC, and designated DOD activities.

(2) Supplement CI and security support resources organic to other commands (including those at ECB) with technical skills, advice, and assistance.

(3) Establish priorities for INSCOM intelligence and security support to OPSEC support programs in accordance with Army regulations and HQDA tasking. Conflicts in priorities between INSCOM and another MACOMs will be referred to HQDA for resolution.

(4) On request, assist in the development of comprehensive OPSEC programs to include evaluating the OPSEC plan of the supported command.

(5) On request, validated per INSCOM procedures, provide Operations Security Evaluations (OSEs) and Project Security Analyses (PSAs) to supported commanders for critical or sensitive facilities, activities, or programs.

(6) Advise and assist Army commanders in electronic warfare (EW) matters and provide technical support to manipulative electronic deception (MED) activities that relate to OPSEC.

(7) Maintain continuous contact with the Army Staff and other supported commands and activities, provide OPSEC advice and assistance, assist in identifying appropriate OPSEC support requirements, and interface for coordinating support programs.

(8) Provide liaison personnel to those Army commands and activities requiring frequent technical assistance in intelligence and security matters.

(9) Ensure compliance with all regulatory policies governing the conduct of intelligence activities by personnel assigned to or under the operational control of INSCOM.

d. CG, USAIA. The CG, USAIA will—

(1) Provide all-source threat evaluations of foreign intelligence and terrorist organizations that threaten the security of the U.S. Army.

(2) Prepare multidiscipline threat data pertaining to SIGINT, EW (less MED and electronic counter-countermeasures (ECCM)), HUMINT, and IMINT for inclusion in OPSEC training programs of the supported commands.

e. Supported commanders. These commanders will—

(1) Comply with command OPSEC program requirements in AR 530–1.

(2) Ensure that supporting MI elements are given all data relating to the organization and activities of the unit needed to support the OPSEC mission.

f. Organic MI elements at ECB. These elements are responsible, within resource capabilities and regulatory guidance, for the OPSEC support to activities of their commands. Organic MI elements may request support, advice, and assistance from the INSCOM supporting element, and other CI analysis and production elements as required.

4–5. Support functional activities

The activities below are those functional activities that support the Army and designated DOD OPSEC programs (AR 530–1). In most instances, the requirements for receiving this support and the procedures for the conduct of these activities are governed by separate Army regulations.

a. Continuing CI special agent support.

b. OSEs.

c. PSAs.

d. Multidiscipline threat data development, maintenance, and dissemination.

e. Security support to special access programs (SAPs). (See AR 380–381.)

f. Support to the U.S. Port Security Program. (See AR 380–89.)

g. Automatic data processing (ADP) systems security. (See AR 380–380.)

h. Technical surveillance countermeasures (TSCM). (See AR 381–14.)

i. COMSEC. (See AR 530–2.)

j. Telephone communications security monitoring. (See AR 380–53.)

k. Control of compromising emanations (TEMPEST). (See AR 530–4.)

l. Electronic security (ELSEC). (See AR 530–3.)

4–6. Continuing CI special agent support

a. An INSCOM CI special agent at the local level acts as liaison between INSCOM and all Army elements receiving intelligence and security support from INSCOM for command OPSEC programs. This special agent either provides the required intelligence and security support directly or assists the supported unit in obtaining needed support that is beyond his or her direct capability.

b. Special agents are the key element in effective CI and security support to OPSEC. They know the threat and vulnerabilities of the supported unit, and are familiar with available support programs and countermeasures. They can, therefore, provide valuable advice and assistance pertaining to the supported unit's needs.

c. A special agent may be designated to support a number of general activities on a given installation or in a given geographic area, or the agent may provide dedicated support for a specific project or exercise for either short- or long-term periods. The method of allocation is tailored to the support needs and nature of Army units in a given locale.

d. Duties of the special agent include, but are not limited to the following:

(1) Providing direct intelligence and security support within his or her capability to include threat assessments.

(2) Advising on availability and feasibility of additional support and countermeasures, and providing assistance in obtaining the necessary support.

(3) Conducting liaison with local, State, Federal, and host country agencies for intelligence information and threat data.

(4) Providing assistance in developing and reviewing command OPSEC.

4–7. Operations security services

OSS are a variety of tailored, multidiscipline intelligence services designed to evaluate and contribute to the OPSEC program of the supported command. OSS are those activities listed in paragraph 4–5*f* through *l*, plus other CI services developed to assist the supported command in strengthening its OPSEC program. The basic level in determining OSS requirements is interface between the supported command and the responsible INSCOM unit, which has many [illegible] See AR 530–1.

4–8. Multidiscipline threat data development, maintenance, and dissemination

a. The development, maintenance, and dissemination of multidiscipline threat data should be ongoing. In order to meet the needs of the supported commander, there must be a continuous application of the intelligence cycle (FM 34–1), to provide information on the multidiscipline and terrorist threat.

b. The focal point for this support is the local CI special agent. Additional comprehensive threat analysis and intelligence support may be obtained from the USAIA per AR 381–11 and AR 381–19.

c. A major component of this aspect of OPSEC support is the multidiscipline threat briefing. Briefings can be tailored, both as to scope and classification level, to familiarize supported commands with the nature of the HUMINT, SIGINT, and IMINT threat posed against the command or activity. Frequently, multidiscipline threat briefings can be combined with required SAEDA briefings presented under AR 381–12.

4–9. Automated Data Processing Systems Security Enhancement Program (ADPSSEP)

The purpose of the ADPSSEP is to preserve the availability, integrity, and confidentiality of Army computer resources and computer-based systems. The ADPSSEP provides services that are scheduled, conducted, and reported under AR 380–380.

4–10. Technical surveillance countermeasures

The TSCM program is conducted in sensitive areas to prevent or detect, nullify, and isolate clandestine monitoring systems, technical security hazards, and physical security weaknesses in accordance with AR 381–14.

4–11. Counter-signals intelligence (counter-SIGINT)

The term counter-SIGINT is used to distinguish between CI activities to support signals security (SIGSEC) and SIGSEC itself.

a. SIGSEC includes COMSEC (AR 530–2) and ELSEC (AR 530–3). It includes all measures taken by a command to prevent exploitation of Army communications-electronics by hostile intelligence. SIGSEC is closely related to command, control, and communications countermeasures, electromagnetic cover and deception, and ECCM (AR 105–86). Counter-SIGINT is intelligence support to a command's SIGSEC program.

b. Counter-SIGINT consists of four primary support functions: threat assessments, vulnerability assessments, countermeasures recommendations, and countermeasures evaluations. The counter-SIGINT support process described in FM 34–6Z applies at all echelons and should be used as the basis for [illegible] at CONUS EAC and FEC.

c. INSCOM CI elements are assigned missions to perform certain regulatory functions that are closely related to counter-SIGINT in support of the overall Army operations and signal security program. These include—

(1) Approving cryptofacilities. The CG, INSCOM is responsible for approving new, relocated, or modified Army fixed cryptofacilities. (See AR 380–40 and the TB 380–41 series.)

(2) Inspecting cryptofacilities. The CG, INSCOM must periodically inspect Army cryptofacilities to ensure that COMSEC material is properly protected, accounted for, used, stored, distributed, and maintained. (See AR 380–40 and the TB 380–41 series).

(3) Evaluating compromising emanations control measures. INSCOM CI elements with appropriately qualified personnel support the Army Compromising Emanation Control Program (AR 530–4), usually referred to as the TEMPEST program. The level of support may consist simply of recommending appropriate TEMPEST countermeasures or could include instrumented TEMPEST tests to determine the existence and strength of compromising emanations (TB 380–7).

(4) Monitoring Army telecommunications. COMSEC monitoring (AR 380–53) and analysis may support the countermeasures evaluation phase of the counter-SIGINT process. Monitoring should never be conducted separately from the counter-SIGINT process. An evaluation based on monitoring alone would be misleading since only a very small sample of a command's telecommunications can be collected and analyzed.

4–12. Hostile intelligence simulation (Red Team)

a. At the request of a supported Army command or agency, INSCOM CI personnel may plan and execute a simulation of a hostile intelligence attack on a specified target (such as headquarters, installation, operation, or program). Such simulations are informally known as "Red Team evaluations." The number of Red Team evaluations is extremely limited due to their complexity and high resource requirements. As a result, they are conducted principally on SAPs and similar sensitive activities.

b. Red Team evaluations may take a multidisciplinary approach, in other words, simulate hostile HUMINT, SIGINT, and IMINT collection and analytical activities against the target. The objective of the Red Team operations is to provide a supported command or agency a realistic tool with which to evaluate internal OPSEC programs. To this end, hostile intelligence simulations should be carried out as realistically as possible, but within the provisions of AR 381–10.

4–13. Special access programs

The CG, INSCOM is responsible for [illegible]

developing and maintaining the attendant capability, methods, and expertise to meet Army requirements. INSCOM will provide, as directed by the Office of the Assistant Chief of Staff for Intelligence (OACSI), life cycle support to SAPs approved by the Secretary of the Army. Such support will be in accordance with AR 380–381.

a. SAPs generally involve either a sensitive military commodity or military operation. In many cases, defense contracts may be involved. The support rendered by INSCOM to SAPs may thus extend to both Government and industrial security enhancements and to the full range of Army research, development, acquisition, and sensitive operational activities for which DA is either proponent or the executive agent.

b. INSCOM activities in support of SAPs will generally include—

(1) Preliminary assessments of the OPSEC posture of proposed SAPs. These assessments are prepared in conjunction with the process of initial approval of a SAP per AR 380–381. They are intended as decision-making aids for the Special Access Program Oversight Committee, HQDA, and the Army leadership.

(2) Periodic reassessments of the OPSEC posture of existing SAPs. These assessments, similar in scope and intent to the preliminary assessments discussed in (1) above, are prepared in conjunction with annual SAP revalidations required by AR 380–381, or at other times as directed by OACSI.

(3) Advice and assistance to SAP proponents. INSCOM will advise and assist, as directed by OACSI, the proponent command or agency of a SAP in the areas shown below.

(a) Organizing and structuring an effective OPSEC program.

(b) Developing classification guides.

(c) Security planning.

(d) Technical assistance and services.

(e) Hostile intelligence simulations.

(4) Termination of SAPs. When SAP status for a program is terminated, INSCOM assistance may be required to ensure an orderly transition to traditional security programs; and, in some cases, to provide continued special protection for residual aspects of completed or cancelled programs.

4–14. OPSEC support to ECB

Organic elements of the Combat Electronic Warfare Intelligence (CEWI) battalion/group, and designated MI units, are the elements within the Army's tactical force structure responsible for providing direct OPSEC support to U.S. Army units at corps and below where these resources exist. These support elements should provide CI and SIGSEC service support to OPSEC less specialized technical services.

Chapter 5
Counterintelligence Production

5–1. General

a. The publication and reporting of CI information to meet intelligence needs takes place at all levels. This chapter provides guidance for CI analysis and production provided by CG, USAIA in support of the Army and other DOD and national agencies.

b. To the maximum extent possible, information from all intelligence collection disciplines (HUMINT, SIGINT, and IMINT) will be used to develop a complete analysis of foreign intelligence and terrorist activities and threats.

5–2. Production objectives

The objectives of Army CI production are to—

a. Collate, analyze, and evaluate information of CI significance.

b. Prepare studies, estimates, and analyses of foreign intelligence services, the activities of terrorists, and related security threats.

c. Support Army security programs by studies and analyses of the total intelligence threat posed to the Army by foreign intelligence services.

d. Support contingency planning and major exercises.

e. Provide analysis and summary of hostile collection and terrorist activities by geographic areas.

f. Participate fully, and represent Army interests, in DOD and intelligence community CI production planning committees and working groups.

5–3. Types of production

The objectives in paragraph 5–2 are met by publication of the following:

a. Current CI information, consisting of raw or partially evaluated perishable data that must be expeditiously disseminated.

b. CI threat analyses tailored to specific activities, units, installations, programs, or geographic areas.

c. CI studies to support contingency planning and major exercises.

d. CI analyses and studies in support of requirements from—

(1) HQDA, MACOMs, and other valid Army requestors.

(2) Director of Central Intelligence.

(3) The Deputy Under Secretary of Defense for Policy.

(4) Defense Intelligence Agency (DIA), acting for the Joint Chiefs of Staff.

(5) Other agencies within the national intelligence community.

e. Studies dealing with the organization, methods of operation, personnel, and activities of foreign intelligence services that pose a current or potential threat to the Army.

f. Analyses and estimates of intelligence on the organization, location, funding, training, operations, capabilities, and intentions of terrorist organizations.

g. Analyses of trends to permit integration of pertinent information into the Army's SAEDA program under AR 381–12.

5–4. Access to and dissemination of existing CI information

a. USAIA will provide current CI information to supported MACOM commanders as required and within resource constraints.

b. USAIA maintains a data base to support CI analysis and production requirements. Requests for intelligence production requirements, which do not need to be, or cannot be satisfied in less than 30 days, may be submitted to Commander, USAIA, ATTN: AIA–PD, WASH DC 20310–1001, per AR 381–19. Send an information copy to Commander, USAITAC, ATTN: AIAIT–KM, BLDG 203, STOP 314, Washington Navy Yard, WASH DC 20374–2136.

c. CI requirements that must be satisfied in less than 30 days may be submitted directly to USAITAC, with information copies to HQDA (DAMI–CIC), WASH DC 20310–1054, and to Commander, USAIA, ATTN: AIA–PD, WASH DC 20310–1001.

5–5. MACOM-level production

Information copies of all CI production within the MACOM will be provided to HQDA (DAMI–CIC), WASH DC 20310–1054, and USAITAC (AIAIT–KM), Bldg 203, STOP 314, Washington Navy Yard, WASH DC 20374–2136.

Chapter 6
Counterintelligence Collection

6–1. General

a. The collection and reporting of information of a CI nature is a continuing requirement for all Army CI elements.

b. National-level collection requirements for CI information are validated and issued by DIA. These consist of—

(1) Intelligence collection requirements.

(2) Continuing intelligence requirements.

(3) Source-directed requirements.

6–2. Identifying and validating collection requirements

Guidelines for validating collection requirements for counter-intelligence information are in DIAM 58–11.

6–3. Collection and reporting procedures

a. All Army CI elements will collect and report military and military-related FI and CI information on the foreign aspects of narcotics production and trafficking in accordance with intelligence collection responsibilities (validated collection requirements), assigned priorities, and resource capabilities.

b. Collection of information on U.S. persons to satisfy legitimate CI needs is authorized when the criteria in AR 381–10,

Procedure 2, are met. This includes the situations in (1) through (4) below. (The detailed criteria in AR 381–10, Procedure 2, paragraph C, should be reviewed before information on U.S. persons is collected and reported.)

(1) When U.S. persons are reasonably believed to be engaged in intelligence activities on behalf of a foreign power.

(2) When U.S. persons are reasonably believed to be engaged in international terrorist activities.

(3) When necessary for the protection of the physical security of Army and Army contractor installation, if such protection is within the assigned mission of the collecting agency.

(4) When the U.S. person is reasonably believed to jeopardize an intelligence operation.

c. CI information responsive to collection requirements will be reported in IIR format using DD Form 1396 (Department of Defense Intelligence Information Report) or message equivalent. Format details are prescribed in DIAM 58–13, part one, chapter 1. Dissemination is limited to headquarters and organizations having a direct interest in the information, and to CI production organizations. In all cases, the original IIR will be sent to DIA, with an information copy to CDR USAITAC AHS VA//AIAIA–KM//. When sensitivity of the information dictates, reporting CI elements may invoke the ORCON caveat per DCID 1/7 to ensure restricted dissemination.

Chapter 7
Liaison and Coordination

7–1. General

This chapter sets forth policy for liaison and coordination with the FBI, Department of Justice, and other Federal, State, and local agencies in matters related to Army CI and security support activities.

7–2. Policy

Effective and continuing liaison with other agency members of the intelligence community, host and other foreign government intelligence agencies, and law enforcement agencies is essential to CI support programs. Commanders of CI elements charged with a liaison responsibility will ensure that it is properly carried out.

7–3. Responsibilities

a. Within the United States—

(1) The CG, INSCOM will maintain continuous liaison with the FBI and other Federal, State, and local agencies to include USACIDC, and will represent the Army at liaison meetings and conferences pertaining to CI matters.

[redacted]

law enforcement authorities is discerned, MACOM commanders will establish a formal Memorandum of Understanding (MOU) with the CG, INSCOM. Use or dissemination of information gathered through liaison must comply with AR 381–10.

b. In overseas areas, MACOM commanders will establish effective liaison programs with other U.S. and foreign agencies, consistent with the following:

(1) Liaison will be conducted by MI units with area responsibilities at EAC.

(2) Tactical MI units are authorized to conduct liaison with local level police and security agencies when such liaison coverage is not available from area support MI units on a regular and timely basis. Such local liaison will be limited to matters specifically within the operational jurisdiction of the tactical MI unit.

(3) To avoid confusion and duplication, intelligence components that desire liaison with foreign agencies will first determine if some other component is performing the needed liaison. If so, attempts should be made to obtain the desired data through agencies with existing liaison.

c. When CI and security cases are under consideration for prosecution by civil authorities, the Office of The Judge Advocate General and the Office of the General Counsel will be notified promptly so they may coordinate with the Department of Justice and U.S. Attorneys in the investigation and prosecution of the cases. Notification will be via electrical message to HQDA WASH DC//DAMI–CIC//.

7–4. Liaison and coordination with the FBI

a. OACSI is the DA liaison agent with the FBI for CI and security matters. Except as provided in this regulation, or as otherwise authorized by OACSI, communications with the national headquarters of the FBI, Washington, DC, concerning such matters will be handled through OACSI.

b. The CG, INSCOM will maintain continuous liaison with the FBI national headquarters and, acting for OACSI, will receive and disseminate, within the Army, FBI reports of security interest.

c. If, during the course of CI operations or investigations, evidence of a crime or intelligence activity surfaces that is within the jurisdiction of the FBI, this information will be provided expeditiously to the local FBI representative and HQDA (DAMI–CIC). Evidence of hostile intelligence activity, developed during the course of a USACIDC investigation and that is outside Army jurisdiction, will be reported to the FBI through the local Army CI component. Additionally, the suspected violation of any Federal [redacted]

Chapter 8
Employment, Use, and Special Administration of U.S. Army Counterintelligence Personnel

8–1. Applicability

This chapter applies to the following:

a. Active Army commands to which CI personnel are assigned.

b. Personnel with SSI 36A or 36B, or MOS 971A, 972A, 97B, or 97C as a primary or additional speciality, or those who are assigned to duties in those specialties.

c. Army civilian employees assigned to investigative/operational duties in CI units. This includes employees in the Military Intelligence Civilian Excepted Career Program (MICECP).

8–2. Use of CI personnel

a. General.

(1) U.S. Army CI special agents are specially trained to perform the following:

(a) Detect and investigate espionage as defined in 18 USC 792–798; sabotage as defined in 18 USC 2151–2156; treason as defined in 18 USC 2381; sedition as defined in 18 USC 2384–2390; and criminal subversion as defined in 18 USC 2387.

(b) Initiate action with military or civilian law enforcement agencies, when appropriate, to prevent and neutralize the threat posed to U.S. Army commands, personnel, and functions by these activities.

(c) Provide CI support to the OPSEC process in Army commands and agencies.

(2) The principles, techniques, and procedures employed in CI investigations, support functions, and operations are outlined in this regulation, AR 381–10, and AR 381–47.

b. Assignment of CI personnel. CI personnel with the primary SSIs/MOSs listed in paragraph 8–1*b*, and U.S. and foreign civilian employees assigned to operational duties in CI units should be assigned to duties and activities that aid the CI effort. This however, does not prohibit assignments to other duties that would broaden the person's experience and enhance advancement potential. Assignment to consecutive tours in noncounterintelligence-related positions may be made only with the approval of the Officer Personnel Management Directorate or Enlisted Personnel Management Directorate, U.S. Army Military Personnel Center (MILPERCEN).

c. Limitations of duties. The use of CI personnel for essential military functions, except as described in this subparagraph, is not prohibited. However, such use should be decided by local commanders in consonance with the policy of denying a potential enemy routine access to the identity of CI personnel. Personnel assigned to positions in operating units, authorized an SSI or MOS as listed in paragraph 8–1*b*, and [redacted]

or preclude accomplishment of essential CI functions.

(2) Will not be used to perform the following:

(a) Investigations of war crimes, atrocities, criminal activities other than those under CI jurisdiction, moral turpitude, welfare of the civilian populace, command, and administrative investigations under AR 15–6 and AR 380–5, or other similar activities, unless such investigations contribute directly to the CI mission, except for internal investigations required by the MI unit to which they are assigned.

(b) Interrogation or detention duties not connected with assigned missions and functions of the unit to which assigned.

(c) Combat patrols and reconnaissance activities, unless CI targets are involved.

(d) Guard or duty officer-type duties, except as required by the MI unit to which they are assigned.

(e) Housekeeping or other duties of a similar nature, except for those required by the MI unit to which they are assigned.

8–3. Security provisions

a. General.

(1) *Dissemination.* Information concerning the following, even if unclassified, is considered operationally sensitive and will be given out only on a strict need-to-know bases:

(a) The internal activities and organizations of CI units.

(b) CI operations, to include techniques, methods, and results obtained.

(2) *Publicity.* Release for publication of any information relative to U.S. Army CI investigations or operations will not be made without prior approval of HQDA (DAMI–CIC).

(3) *Debriefing.* When the need-to-know requirements of personnel assigned to CI duties or activities have ceased, the unit commander will have such personnel—

(a) Orally debriefed.

(b) Execute a DA Form 2962 (Security Termination Statement and Debriefing Certificate) in accordance with AR 380–5, chapter 10. This form will be executed before the person is retired or released from active duty, on the withdrawal one of the SSIs or MOSs listed in paragraph 8–1*b*, or at any preceding time judged appropriate by the unit commander. The above does not apply to personnel transferring from one assignment to another when the new assignment will be to CI or related duties.

b. Classification.

(1) Information concerning the matters in *(a)* and *(b)* below will be classified Confidential or higher and marked as follows: Classified by: AR 381–20. Declassify on: (specify date, event, or "OADR").

(a) Plans, sources, methods, activities, and results of CI operations and investigations conducted under the provisions of AR 381–12–1, and para 2–2*b* of this regulation.

(b) Nature of, and use by, CI units of classified nonstandard equipment.

(2) Normally, there is no security classification assigned to identification of CI personnel, such as names, ranks, and duty positions. Such information will be classified only if essential to mission security. If unclassified, it will be protected under the provisions of the Freedom of Information Act as For Official Use Only.

(3) CI special agents in the conduct of CI activities will not be required to reveal their military grade or position other than as "CI special agent" when such disclosure might interfere with the discharge of investigative or operational duties. Their status as a member or employee of the U.S. Army may also be concealed if such concealment is in the best interests of a specific investigation or operation. (See AR 381–10, Procedure 10.)

(4) The authorized and assigned personnel strength of a CI unit is usually unclassified. The personnel strength of a "special mission" CI unit may be classified if knowledge of such information would impair mission accomplishment. Such classification requires the approval of the commander of the MACOM to which the unit is assigned.

(5) Officer and enlisted evaluation reports will be classified Confidential or higher only when they include the following:

(a) A description of classified duties performed, or

(b) Statements of operational proficiency (if classified duties are discussed).

(6) Personnel evaluation reports will be unclassified unless such status inhibits the accurate rating or description of the individual's ability and potential.

(7) This subparagraph does not preclude CI personnel from including in resumes or discussing with prospective employers unclassified information from their backgrounds and from duties performed by them in their assignments.

c. Declassification of classified records. Losing units will—

(1) Screen records of persons with a specialty MOS or SSI listed in paragraph 8–1*b*, when any of the following occurs:

(a) Relieved from active duty.

(b) Discharged from the Service.

(c) Reassigned from duties in CI units to duties in other units.

(2) Declassify records when appropriate.

(3) Withdraw and retire or destroy information that should remain classified in accordance with this regulation and AR 380–5.

(4) Use unclassified orders to effect reassignment of personnel.

8–4. Clothing

a. Personnel assigned to CI duties will wear clothing appropriate to the mission and cover as authorized by the unit commander to which assigned or attached. Personnel authorized to wear civilian attire in accordance with the mission and cover will not be required to perform military functions or attend military formations that would reveal their military status.

b. Enlisted personnel assigned to perform duties requiring the wearing of civilian clothing are entitled to the allowances prescribed under the procedures in AR 381–141.

8–5. Nonstandard spectacles

Issue of nonstandard spectacles to personnel assigned to MOS or SSI positions listed in paragraph 8–1*b* is authorized by AR 40–3.

8–6. Access to military privileges

CI personnel required to wear civilian clothing have medical, exchange, commissary, and other normal military privileges to which they are entitled as members of the armed forces. When required for security purposes, local procedures will be established that will permit such personnel access to above noted services, on presentation of agreed-on identification. This may include the issue of identification cards bearing the title "special agent" in lieu of military or civilian grade. (Such cards will be turned in on transfer of the individual to whom issued.) When required to protect the rights and benefits of persons concerned, essential elements of identification, properly classified, will be made a matter of record between intelligence unit commanders and agencies concerned. Thereafter, grade and unit to which assigned will not be required as elements of identification. Such elements of identification will be given limited dissemination on a need-to-know basis only. Documents involved will be classified, if required, in accordance with this paragraph.

8–7. Billets and messes

a. Enlisted CI special agents assigned to special agent duties will not be billeted in normal troop-type billets. When warranted by the nature of official duties, as certified by their commander, CI special agents will be authorized to reside offpost and will be entitled to allowances commensurate with their grade (AR 210–11).

b. Enlisted CI special agents performing investigative or operational duties in a temporary duty (TDY) status will not be billeted in troop transient billets. TDY orders will reflect that use of Governmental mess and billeting facilities would be detrimental to the mission, if such disclosure might interfere with sensitive investigative or operational duties.

c. Enlisted CI special agents will be authorized rations not available (RNA) under the provision of the DOD Military Pay and Allowances Manual, chapter 1, part 3.

d. The provisions in *(a)* through *(c)* above apply in overseas areas except in those areas not authorized basic allowance for quarters and RNA.

8–8. Oath administration

a. In the performance of investigative duties authorized by this regulation, a CI special agent on active duty in the Army is authorized to administer oaths when taking

statements. The agent's title for the purposes of administering oaths is "Counterintelligence Special Agent, U.S. Army". (See the Uniform Code of Military Justice, Article 136*(b)*.)

b. An Army civilian employee who is assigned to investigative or operational duties in a CI unit is authorized by 5 USC 303*(b)* to administer oaths when taking statements as part of an official investigation. This includes Army civilians in the MICECP. The employee's title for the purposes of administering oaths is "Counterintelligence Special Agent, U.S. Army."

8–9 . Freedom of movement

a. During the course of a CI investigation or operation, CI special agents are authorized freedom of movement between geographical areas of responsibility.

b. CI personnel assigned to the Foreign Counterintelligence Activity, INSCOM, are not required to obtain specific theater clearance from overseas commanders prior to undertaking overseas travel in connection with their official duties. (See AR 1–40, para 1–2*b(5)*.) The senior intelligence officer of the Army theater will be notified in advance of such travel, or as soon as possible thereafter, if circumstances preclude advance notification.

8–10. Weapons

CI personnel may carry weapons openly or concealed as required in the performance of official duties, when authorized by a CI commander or supervisor of field grade or higher rank. Written authorization, using DA Form 2818 (Firearms Authorization), is required for carrying a weapon and will be carried at all times by CI personnel when armed. If the weapon is authorized to be concealed, the DA Form 2818 will so state. CI commanders will ensure the individual has met the requirements of AR 350–4 and the qualifications/familiarization requirements of AR 190–14.

8–14. Apprehension authority

MI special agents who are officers or noncommissioned officers, and intelligence component employees of DOD who are authorized to carry badges and credentials, have the authority to apprehend persons subject to the Uniform Code of Military Justice in connection with investigations into national security offenses over which MI has investigative jurisdiction (para 2–2), provided that such agents have a probable cause to believe that an offense has been committed and that the person to be apprehended committed it.

8–12. Involvement in civilian legal proceedings

Requests for the appearance of CI personnel as depositions or in civil proceedings and for the subpoena of information exempt from [illegible]

Chapter 9
U.S. Army Intelligence Badges and Credentials

9–1. General

This chapter—

a. Establishes policies and procedures for the procurement, issue, control, and disposition of U.S. Army intelligence badges and credentials.

b. Applies to all active U.S. Army MI units and to personnel authorized to use U.S. Army intelligence badges and credentials.

9–2. Responsibilities

a. The ACSI—

(1) Exercises general staff supervision over and establishes policies regarding the procurement, manufacture, issue, use, and disposition of badges and credentials and associated items.

(2) Provides guidance to enable the CG, INSCOM to procure, store, issue, and dispose of badges and credentials.

b. The CG, MILPERCEN—

(1) Notifies the CG, INSCOM of the award or withdrawal of the SSIs/MOSs listed in paragraph 8–1*b*.

(2) Furnishes copies of assignment orders or instructions on above personnel.

c. The CG, INSCOM—

(1) Manages the U.S. Army intelligence badge and credential program.

(2) Exercises supervision over the storage, accounting for, issue, and disposition of badges, credentials and credential forms (DA Forms 3363, and 3363–1 (U.S. Army Intelligence Credential) and DA Form 3363–A (U.S. Army Intelligence Credential (Representative)).

(3) Operates the central repository for badges, credentials, and credential forms.

(4) Manages the badge trophy program.

d. MI unit commanders—

(1) Control and safeguard badges, credentials, and credential forms charged to their unit in accordance with this regulation.

(2) Appoint badge and credential custodians, subcustodians, and their alternates. When possible, custodians, subcustodians, and alternates will possess an intelligence MOS.

e. Custodians, alternate custodians, subcustodians, and alternate subcustodians receive and issue badges and credentials. They are the only persons authorized to receipt for badges.

f. The CG, U.S. Army Intelligence Center and School (USAICS)—

(1) Performs initial processing of credentials for school attendees.

(2) Informs the CG, INSCOM when persons are dropped from courses at USAICS.

g. Persons issued badge and credentials—

(1) Are responsible at all times for safeguarding their badge and credentials unless properly relieved of this responsibility by the custodian, subcustodian, or an alternate.

(2) Are responsible to become familiar with [illegible]

9–3. Use of badges and credentials

a. Badges and credentials are for the sole purpose of identifying the bearer as a duly accredited special agent or representative of U.S. Army intelligence who is performing official intelligence duties. Their use for other than official duties, or when other means of identification would suffice, is sufficient basis for disciplinary action and removal from investigative duties.

b. Only credentials prepared on DA Forms 3363, 3363–1, and 3363–A are valid U.S. Army intelligence credentials.

c. The falsification, forgery, alteration of, or tampering with intelligence badges or credentials is prohibited. Photographing or otherwise copying badges or credentials, as well as willful misuse, is also prohibited. Violations of these provisions may result in administrative or criminal penalties as prescribed by law and regulation.

9–4. Channels of communication

U.S. Army intelligence badges and credentials will be produced by the CG, INSCOM and shipped to custodians. Unless otherwise indicated herein, all correspondence concerning badge and credential procurement manufacture, accountability, storage, shipment, withdrawal, and destruction will be addressed to the CG, INSCOM, ATTN IAOPI-BC, Fort Meade, MD 20755-5900.

9–5. Criteria for issuance

a. DA Forms 3363 and 3363–1 are issued to the following personnel who are at least 21 years of age:

(1) Military personnel on active duty with MI units for over 2 weeks who hold CI investigative SSIs/MOSs as listed in paragraph 8–1*b*, and who have attended the CI course at the USAICS, or USAI equivalent.

(2) Military personnel with the above SSI/MOS on active duty for over 2 weeks in a nonintelligence unit, but performing CI investigative duties.

(3) Civilians employed with the MICECP performing CI investigative duties.

(4) Other Army civilian investigators who are assigned CI investigative duties under U.S. Army cognizance.

(5) ARNG and USAR CI personnel who are performing CI duties in conjunction with Active Army CI units, on approval of the CG, INSCOM and for the duration of specific mission. When not being used badges and credentials of USAR CI personnel will be held by the appropriate active Army CI unit custodian or subcustodian.

b. DA Form 3363–A may be issued to the following personnel whose intelligence duties require unique identification that cannot be provided by other means (for example, military identification card; or letter of introduction):

(1) MI personnel who hold Army intelligence SSI 36B, MOS 97A or 97C assigned to HUMINT [illegible]

(2) Civilian employees (including MICECP) assigned to HUMINT duties.

(3) Foreign national employees of MI units assigned to investigative duties.

(4) Target exploitation (TAREX) personnel, when such identification is necessary for the conduct of official duties.

9–6. Special issue of credentials

a. Under exceptional circumstances, personnel other than those identified in paragraph 9–5, who are performing intelligence or intelligence-related duties, may request representative credentials. A detailed justification of the exceptional circumstances must be submitted through the MACOM with the request and will be signed or endorsed by the commander of the MI group or separate MI element to which the individual is assigned.

b. Requests will include name, grade, SSI/MOS (or civilian job series), and Social Security Number (SSN). Requests are subject to the approval of the CG, INSCOM or his designated representative. Disapproved requests will be returned.

9–7. Issuance procedures

a. Active Army units having personnel who require use of badges and credentials in the performance of official intelligence or counterintelligence duties must first establish a custodian account with the commander, INSCOM, ATTN: IACI–BC Fort Meade, MD 20755–5900, unless one has already been established by a parent unit. A letter request will be submitted through channels, identifying the unit, the number of personnel requiring badges and credentials, and the nature of the mission or duties requiring such identification. The letter will include correct mailing and message addresses for the custodians, their telephone numbers, and a copy of appointment orders for the custodian and alternate custodian.

b. Once the account is established, subsequent communications will be directly between the custodian and the badge and credential controller.

c. Sub-custodians and alternate sub-custodians will be appointed as necessary to ensure continuous control and receipting between the parent (custodian-level) unit and any subordinate elements.

d. USAR units using badges and credentials in support of or to assist Active Army intelligence or CI programs will obtain them through the Active Army custodian.

e. Badges and credentials for authorized personnel will be obtained by the custodian in the following manner:

(1) Submit letter or message request to the badge and credential controller (para 9–4), with full identifying data, citing authority for issue and providing justification if required (paras 9–5 or 9–6).

(2) Two color photographs, head and shoulders, in civilian business dress, large enough to be cut to size 1 by 1¼ inches, will be forwarded as an enclosure to the request; if badge and credentials were not previously manufactured. If instant development-type photographs are used, do not mount them on stiff backing.

(3) On receipt of the color photographs, the badge and credential controller will forward a blank DA Form 3363–1 to the requesting unit with instructions to have the individual for whom the badge and credentials are intended sign the blank form. No other person may sign the form. A legible payroll signature will be made with a ballpoint pen (black ink) in the appropriate portion of the form.

(4) The signed credential form will be returned to HQ, INSCOM within 10 working days for manufacture of the credentials.

9–8. Safeguard and control

a. Storage. When in storage, badges, credentials, and credential forms will be properly secured to guard against loss, theft, or unauthorized use. These items will be locked in a security container that meets the requirements of AR 380–5, paragraph 5–101.

b. Correspondence. Routine correspondence concerning badges and credentials, badge and credential numbers, and names of individuals to whom issued is unclassified. However, such correspondence that lists personal identifying data (for example, name, SSN, and date and place of birth) of individuals requiring credentials shall be marked For Official Use Only. The For Official Use Only caveat will serve to indicate that such information may be exempt from the public disclosure provisions of the Freedom of Information Act.

c. Temporary surrender.

(1) The badge and credentials will be surrendered to the appropriate custodian, subcustodian, or alternate custodian/subcustodian, as appropriate, if the individual to whom they are issued is—

(a) Hospitalized.

(b) On leave in excess of 72 hours.

(c) Placed in a temporary noninvestigative status for any reason.

(d) Planning to cross international boundaries on other than official business.

(e) Expected to be placed in a situation where loss of badge and credentials is likely.

(2) The badge and credentials will be reissued to the member on return to investigative duties.

d. Surrender means. In circumstances where the surrender of badge and credentials (*c*) above would involve mailing them or otherwise increase the risk of loss (for example, a one-man office), the CG, INSCOM may approve alternate procedures.

e. Individual safeguards. Individuals issued a badge and credentials will appropriately and reasonably safeguard them at all times to preclude their loss or theft.

f. Permanent surrender. The badge and credentials of persons involved in the following personnel actions will be returned to CG, INSCOM (at the address in para 9–4) within 2 working days after the date the action is effective:

(1) Transfer to a unit having no requirement for intelligence investigative personnel.

(2) Permanent assignment to noninvestigative or non-HUMINT duties with an Army intelligence unit.

(3) Withdrawal of SSIs/MOSs listed in paragraph 8–1*b*.

(4) Relief or retirement from active duty.

(5) Termination of USAR CI personnel affiliation with an Active Army CI unit if issued badges and credentials under paragraph 9–5*a*(5).

(6) Resignation by an Army civilian employee.

9–9. Accountability

a. On change of custodian or subcustodian—

(1) A joint inventory of badges, credentials, and credential forms will be conducted by the old and new custodians or subcustodians. Such inventories should be made sufficiently in advance to allow verification and clarification of discrepancies prior to the departure of the old custodian/subcustodian.

(2) Items will be listed in numerical sequence on DA Form 2496 (Disposition Form). The DA Form 2496 will be prepared in duplicate and contain the following statement: "A joint inventory of all badges and credentials assigned to the (name of unit) was conducted on (date) by (name of old custodian/subcustodian) and (name of new custodian/subcustodian). All badges, credentials and credential forms listed below are in serviceable condition. As of (date), I assume full responsibility as the unit badges and credentials custodian/subcustodian."
(Signature of the new custodian/subcustodian)

(3) Inventories, together with two copies of the orders appointing a new custodian, will be forwarded to the address in paragraph 9–4. On verification of the inventory, the Badge and Credentials Controller, HQ, INSCOM will sign the duplicate copy of the inventory and return it to the unit. This completely relieves the old custodian of accountability. The original of the inventory will be retained by CG, INSCOM.

(4) Change-of-subcustodian inventories, together with two copies of the DA Form 2496 appointing the new subcustodian, will be forwarded to the parent unit custodian. Custodians will complete verification procedures as described in *a* above.

b. Badge and credentials custodians will conduct an inventory of all badges, credentials, and credential forms assigned to their custody during the first work week in January and July, each year. Results of the inventory will be forwarded to the CG, INSCOM no later than the last day of January and July. Results of the inventory will be submitted in a format similar to that in *a* above. Subcustodians will also conduct semiannual inventories. They will forward the results to the parent unit custodian in time

to allow the custodian to comply with this paragraph.

c. Badges, credentials, and credential forms are accountable on a continuous receipt system at all times. MI unit commanders, badge and credentials custodians/subcustodians, alternate badge and credentials custodians/subcustodians, and individuals to whom badge and credentials are issued, will ensure use of this system. A similar system will be kept on registered packages of badges, credentials, and credential forms.

d. DA Form 4354–R (U.S. Army Intelligence Badge and Credentials Receipt and/or Tracer) will be used to maintain a continuous receipting system for all badges, credentials, and credential forms.

(1) Shipment of badges, credentials, and credential forms will be in accordance with paragraph 9–12.

(2) The issuing custodian or subcustodian will maintain the signed DA Form 4354–R until the badge and credentials are surrendered. At time of surrender, the form is to be annotated (relieving the individual of accountability). A copy of the annotated form will be furnished to the individual.

(3) A copy of DA Form 4354–R is located at the back of this regulation. It will be reproduced locally on 8– by 11–inch paper.

9–10. Initial processing of USAICS attendees for credentials

Initial processing of individuals for credentials will be done at USAICS. The names of those attending courses awarding SSI 36A, or MOS 971A and 97B will be forwarded from USAICS to INSCOM within 4 weeks after the start of the appropriate class. USAICS will also forward the names of members who have been dropped from these courses so that credential processing can be stopped and original lists corrected.

9–11. Reissue

Requests for reissue of badge and credentials will be forwarded directly from custodians to the CG, INSCOM by the fastest means available when authorized personnel are assigned to, or arrive on station. Requests should include the name, SSN, and, if known, the badge and credentials number of the individual.

9–12. Shipment

Badges, credentials, and credential forms will be shipped by registered U.S. mail or by military courier using DA Form 4354–R. Shipping instructions are given below.

a. Packaging. Regardless of the quantity, badges and credentials shipped by the following methods will be treated as shown:

(1) Registered mail will be packaged with buffer material to prevent damage from internal shifting or external causes. Each package will be doublewrapped with the inner wrapping stamped "To be opened by addressee only." Badges and credentials will not be combined with other registered mail.

(2) Items sent via U.S. military courier will be placed in a double envelope with buffer material if necessary to prevent damage.

b. Shipping from HQ, INSCOM to custodians. The original copy of a DA Form 4354–R (containing the INSCOM return address) for each badge and credential being sent will be enclosed in that shipment. HQ, INSCOM will keep a copy of each form on which will be recorded the registered package number. On receipt of badges and credentials, the unit badge and credentials custodian, or alternate, will sign and return DA Form 4354–R to HQ, INSCOM.

c. Shipment from custodians to HQ, INSCOM. A copy of the reassignment or separation orders of each member concerned and a properly executed DA Form 4354–R containing the return address of the unit will be enclosed in each shipment. A copy of the form on which the registered package number is recorded will be kept to ensure the return of a signed receipt or for tracer action. On receipt of badges and credentials, the Badge and Credential Controller, HQ, INSCOM will sign and return the original DA Form 4354–R to the custodian, along with the original DA Form 4354–R signed by the unit custodian. This relieves the custodian of accountability. In no case will badges and credentials be shipped later than the individual's actual departure date from the unit.

d. Shipping between custodians and subcustodians. Each unit will follow a parallel procedure to *c* above using DA Form 4354–R when badges, credentials, and credential forms are shipped between custodians and subcustodians.

e. Shipping between continental United States units or units in the same overseas command. The badges and credentials of transferred personnel will be shipped by the custodian of the losing unit directly to the custodian of the gaining unit. A copy of the individual's transfer orders, as well as the original copy of DA Form 4354–R, will be enclosed in the badge and credentials shipment to the new unit. This original DA Form 4354–R will be signed by the custodian of the gaining unit and returned to the sender. The gaining custodian will execute a new form in two copies and forward the original to HQ, INSCOM. On receipt, HQ, INSCOM will return to the custodian of the losing unit the signed DA Form 4354–R, thereby relieving him/her of accountability.

9–13. Replacement of unserviceable badges and credentials

a. Inspection. To ensure credentials are in a usable and professional condition, during each inventory (para 9–9*b*), custodians or subcustodians will inspect credentials for damage or obsolescence. Inspections should note cracks, chips, creases, and warping or obsolescence due to any change in facial features. Records of this inspection will be kept in unit files for 1 year or until the soldier departs his or her current assignment.

b. Replacement procedures. When U.S Army intelligence credentials are determined to be unserviceable or must be replaced because of an unusable badge, replacement will be obtained using the procedures for re-issue prescribed in paragraph 9–11. On issuance of the replacement badge and credentials, the old badge and credentials will be returned to INSCOM.

c. Leather holders. Holders for credentials are procured, issued, and mailed with the badge and credentials by HQ, INSCOM. Replacement holders will be furnished by HQ, INSCOM on request Serviceable holders will be returned with the badge and credentials for reissue.

9–14. Central badge and credentials repository

a. HQ, INSCOM holds badges and credentials of authorized personnel whose current duties do not require their use.

b. Badges and credentials for personnel either separated or retired from active duty with U.S. Army intelligence, and whose duties formerly required badge and credentials, will be maintained by HQ, INSCOM Badges will be returned to stock for reissue Credentials will be held for a period of 1. months, then destroyed.

9–15. Badge trophy

All badge-carrying personnel with the SSIs/MOSs listed in paragraph 8–1*b*, or prior service equivalent (this includes MICECP) may obtain, at their own expense, a U.S Army MI badge in trophy form on honorable final separation from the Army, provided their SSI/MOS was not withdrawn for cause. Details concerning this program may be obtained by writing to Director, Foreign Counterintelligence Activity Attn IAFS–RM (B&C) Ft Meade, MD 20755–5986.

9–16. Loss or misuse of badges and credentials

a. The loss or misuse of badges and credentials may be considered a basis for removal of the SSIs/MOSs listed in paragraph 8–1*b*. Immediately upon discovering the loss, the individual accountable for the lost item will notify his or her immediate superior and will conduct an immediate search of the suspected area of loss.

b. On loss of a badge, credentials, or blank DA Form 3363, 3363–1, or 3363–A units will take the following actions:

(1) Notify HQ, INSCOM (at the address in para 9–4) of the loss by the fastest means available.

(2) Begin an immediate search for recovery.

(3) Start an investigation into the circumstances of loss under the provisions of AR 15–6.

(4) As appropriate, notify local and national investigative agencies of the loss. See figs 9–1 and 9–2 for sample notification letters for badge and credentials loss.

c. A copy of the results of the loss or misuse investigation will be forwarded

through command channels to HQ, INSCOM within 30 days of the incident.

d. The report will include a request for relief from accountability from INSCOM for the lost item and a statement of any disciplinary action taken, to include any action taken to remove the responsible individual's SSI/MOS under AR 140–192, AR 614–200, or DA Pam 310–1 as appropriate. Relief from accountability will be granted on satisfactory review of the investigation and any corrective measures.

Appendix A
References

Section I
Required Publications

AR 1–40
Clearance Requirements and Procedures for Official Temporary Duty Travel Outside the Continental United States. (Cited in para 8–9*b*.)

AR 27–40
Litigation. (Cited in para 8–12.)

AR 40–3
Medical, Dental, and Veterinary Care. (Cited in para 8–5.)

AR 105–86
Performing Electronic Countermeasures in the United States and Canada. (Cited in para 4–11*a*.)

AR 140–192
Organization, Training, Assignment, and Retention Criteria for Military Intelligence, Signals Intelligence, Electronic Warfare, and Signals Security Units. (Cited in para 9–16*d*.)

AR 190–14
Carrying of Firearms. (Cited in para 8–10.)

AR 190–52
Countering Terrorism and Other Major Disruptions on Military Installations. (Cited in para 3–3.)

AR 195–6
Department of the Army Polygraph Activitites. (Cited in para 2–3*e*.)

AR 350–4
Qualification and Instructional Firing with Weapons and Weapons Systems. (Cited in para 8–10.)

AR 380–5
Department of the Army Information Security Program. (Cited in paras 8–3*a(3)(b)* and *c(3)*, and 9–8*a*.)

AR 380–40 (C)
Policy for Safeguarding and Controlling COMSEC Information (U). (Cited in para 4–11*c(1)* and *(2)*.)

AR 380–53
Communications Security Monitoring. (Cited in paras 4–5*j* and 4–11*c(4)*.)

AR 380–381 (S)
Special Access Programs (SAPs) (U). (Cited in paras 4–5*e* and 4–13.)

AR 381–10
U.S. Army Intelligence Activities. (Cited in paras 2–2*a* and *h*, 2–3*e*, 4–12*b*, 7–3*a(2)* and 7–4*c*, 8–2*a(2)*, and 8–3*b(3)*.)

AR 381–11
Threat Support to U.S. Army Force, Combat, and Material Development. (Cited in para 4–8*b*.)

AR 381–12
Subversion and Espionage Directed Against U.S. Army (SAEDA). (Cited in paras 4–2*c(2)*, 4–8*c*, and 5–3*g*.)

AR 381–12–1 (C)
Processing of Subversion and Espionage Directed Against U.S. Army Incidents (U). (Cited in para 8–3*b(1)(a)*.) (Distribution of this regulation is limited to active CI units.)

AR 381–14 (C)
Counterintelligence: Technical Surveillance Countermeasures (U). (Cited in paras 4–5*h* and 4–10.)

AR 381–19
Intelligence Support. (Cited in paras 4–8*b* and 5–4*c*.)

AR 381–45
Investigative Records Repository (IRR). (Cited in para 2–4*i*.)

AR 381–47 (S)
U.S. Army Offensive Counterintelligence Operations (U). (Cited in paras 1–6*b(2)*, 2–4*h*, 4–2*c(2)*, and 8–2*a(2)*.) (Distribution of this regulation is controlled by OACSI and is limited to active CI units.)

AR 381–141 (C)
Provisions for Administration, Supervision, Control, and Use of Intelligence Contingency Funds (U). (Cited in para 8–4*b*.)

AR 530–1
Operations Security (OPSEC). (Cited in paras 4–2*b*, 4–4*a* and *e(1)*, 4–5, and 4–7.)

AR 530–2
Communications Security. (Cited in paras 4–5*i* and 4–11*a*.)

AR 530–3 (C)
Electronic Security (U). (Cited in paras 4–5*l*. and 4–11*a*.)

DIAM 58–11 (S–NF)
Defense Human Resources Intelligence Collection Management Manual. (Cited in para 6–2.)

DIAM 58–13
Defense Human Resources Intelligence Collection Procedures. (Cited in para 6–3*c*.)

FM 34–1
Intelligence and Electronic Warfare Operations. (Cited in para 4–8*a*.)

FM 34–62
Counter-Signals Intelligence Operations. (Cited in para 4–11*(b)*.)

TB 380–7 (C)
TEMPEST (U). (Cited in para 4–1*c(3)*.)

TB 380–41
Procedures for Safeguarding, Accounting and Supply Control for SOMCES Material. (Cited in paras 2–4*g*, 4–11*c(1)*, and *(2)*.)

UCMJ
The Uniform Code of Military Justice. (Cited in paras 8–8*a*, and 8–11.)

Section II
Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 15–6
Procedures for Investigative Officers and Boards of Officers Conducting Investigations.

AR 190–47
The U.S. Army Correctional System.

AR 195–2
Criminal Investigation Activities.

AR 210–11
Installation—Billeting Operations.

AR 381–15 (C)
Foreign Military Intelligence Collection Activities Program (U).

AR 604–5
Personnel Security Program.

AR 606–15

Section III
Prescribed Forms

DA Form 4354
U.S. Army Intelligence Badge and Credentials Receipt and/or Tracer. (Cited in para 9–9e.)

Section IV
Referenced Forms

DA Form 2496
Disposition Form.

DA Form 2818
Firearms Authorization.

DA Form 2962
Security Termination Statement and Debriefing Certificate.

DA Form 3363
U.S. Army Intelligence Credential.

DA Form 3363–1
U.S. Army Intelligence Credential.

DA Form 3363–A
U.S. Army Intelligence Credential (Representative).

DD Form 1396
Department of Defense Intelligence Information Report.

Appendix B
Department of Defense Directive 5240.2

Department of Defense Directive

June 6, 1983
NUMBER 5240.2

SUBJECT:
DoD Counterintelligence

References:
(a) DoD Directive 5240.2, "Department of Defense Counterintelligence," December 18, 1979 (hereby canceled)
(b) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(c) DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," December 3, 1982
(d) DoD Directive 5148.11, "Assistant to the Secretary of Defense (Intelligence Oversight)," December 1, 1982
(e) DoD Directive 5000.19, "Policies for the Management and Control of Information Requirements," March 12, 1976

A. Reissuance and Purpose

This Directive:

1. Reissues reference (a).

2. Implements reference (b) as it pertains to the assignment of counterintelligence (CI) responsibilities to the Secretary of Defense and the Military Departments.

3. Establishes and maintains a comprehensive, integrated, and coordinated CI effort within the Department of Defense.

4. Assigns responsibilities for the direction, management, coordination, and control of such activities conducted under the authority of reference (b) and this Directive.

5. Fstablishes the Defense Counterintelligence Board (DCIB).

B. Applicability

This Directive applies to the Office of the Secretary of Defense, the Military Departments the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

C. Definitions

Terms used in this Directive are defined

Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation," between the Attorney General and the Secretary of Defense, April 5, 1979 (hereafter referred to as the "Agreement"), that is, "the systematic collection of information regarding a person or group which is, or may be engaged in, espionage or other clandestine intelligence activity, sabotage, international terrorist activities or assassinations conducted for, or on behalf of, foreign powers, organizations or persons."

2. *Counterintelligence Operations.* The meaning as used in the "Agreement," that is, "actions taken against hostile intelligence services to counter espionage and other clandestine intelligence activities damaging to the national security."

D. Policy

It is DoD policy that CI activities shall be:

1. Undertaken to detect, identify, assess, and counter or neutralize the intelligence collection efforts, other intelligence activities, sabotage, terrorist activities, and assassination efforts of foreign powers, organizations, or persons directed against the Department of Defense, its personnel, information, material, and activities.

2. Conducted in accordance with applicable statutes, E.O. 12333 (reference (b)), and other DoD issuances that govern and establish guidelines and restrictions for these activities. This includes the procedures that are issued under DoD Directive 5240.1 (reference (c)) and that govern, among other things, CI activities that affect U.S. persons.

3. Conducted in accordance with this Directive, other DoD issuances, and the policy, standards, criteria, and operational guidelines established by the Secretary of Defense or designee.

4. Coordinated within the United States in accordance with the "Agreement" (identified in subsection C.1., above) between the Attorney General and the Secretary of Defense, and outside the United States with the Director of Central Intelligence.

5. Inspected in accordance with DoD Directive 5148.11 (reference (d)).

E. Delegation of Authority

The Deputy Under Secretary of Defense for Policy (DUSD(P)), under the direction, management, and control of the Under Secretary of Defense for Policy, is delegated the authority to act for the Secretary of Defense in carrying out CI responsibilities assigned by reference (b).

F. Procedures

To achieve DoD CI

1. Conduct CI investigations to detect and neutralize or prevent espionage activities and detect and resolve incidents of foreign-directed sabotage, terrorist activities, and assassinations.

2. Employ offensive CI operations against hostile foreign intelligence services to identify and exploit hostile agents, lessen the hostile intelligence threat, uncover espionage penetrations of the Department of Defense, and identify hostile intelligence targeting of DoD personnel, information, and resources.

3. Collect, analyze, evaluate, and disseminate information of CI significance; and prepare studies, estimates, and analyses of (a) foreign intelligence services, their organization, methods of operation, personnel, activities, communications, funding, and support and (b) international terrorism and related security threats to DoD interests.

4. Prepare, in support of DoD operations security programs, studies and analyses of the multidisciplinary intelligence threat posed to the Department of Defense by foreign intelligence services, including systems, targeting, control mechanisms, deployment, and capabilities.

G. Defense Counterintelligence Board

1. *Organization and Management*

a. The DCIB shall be chaired by the Director for Counterintelligence and Security Policy, Office of the DUSD(P) (ODUSD(P)). The Director, Counterintelligence and Investigative Programs, ODUSD(P), shall serve as Executive Secretary.

b. The DCIB membership shall include the Assistant General Counsel (International); the Assistant to the Secretary of Defense (Intelligence Oversight); and one representative from each of the Military Department CI components, the Defense Intelligence Agency (DIA), and the National Security Agency/Central Security Service (NSA/CSS).

c. The DCIB shall be supported by subcommittees, with participation from those organizations represented on the DCIB and the OJCS. Chairs of the subcommittees shall be appointed by the Chair, DCIB.

2. *Functions.* The DCIB shall advise and assist the DUSD(P) on CI matters within the purview of E.O. 12333 (reference (b)) and this Directive.

H. Responsibilities

1. The *Deputy Under Secretary of Defense for Policy* shall:

a. Exercise policy supervision over and manage DoD CI programs and activities as defined in this Directive.

b. Establish policies and procedures for the conduct and administration of DoD CI activities.

planning guidance for DoD resources engaged in CI.

e. Act as program manager for DoD resources included in the DoD Foreign Counterintelligence (FCI) Program; review proposed Military Department and DIA CI resource programs for efficiency and effectiveness; formulate budget estimates for the DoD FCI Program; allocate resources to these programs; review costs, budgets, and financial plans; and evaluate the implementation of approved programs.

f. Conduct assessments of the effectiveness of CI support to users, the quality of the CI product, and the effectiveness and efficiency of DoD CI components and systems; review and monitor the progress of offensive CI operations; and approve or refer to the National Security Council (NSC) sensitive operations that involve significant policy issues.

g. Coordinate DoD CI programs and activities with other U.S. Government organizations.

h. Provide staff support to the Secretary of Defense on NSC matters and provide for DoD representation on national, international, and interdepartmental boards, committees, and other organizations involved in CI matters.

i. Conduct, or provide for the conduct of, staff inspections of DoD CI components to monitor established programs.

j. Assign special tasks to DoD Components as may be necessary to accomplish DoD CI objectives.

2. The *Secretaries of the Military Departments* shall:

a. Provide for the conduct, direction, management, coordination, and control of CI activities in accordance with this Directive and E.O. 12333 (reference (b)).

b. Maintain, operate, and manage their respective CI components in accordance with the authorities and responsibilities assigned in this Directive and provide personnel, equipment and facilities that CI tasks require.

c. Establish Military Department plans, programs, policies, and procedures to accomplish authorized CI missions.

d. Establish and maintain a worldwide CI capability for the purposes outlined in subsection D.1., above.

e. Develop CI techniques, methods, and equipment required for CI activities.

f. Provide CI support to other DoD Components, U.S. Government organizations, and foreign CI and security agencies as provided for in this Directive and reference (b).

g. Provide basic and specialized training to CI personnel.

h. Submit CI operational data and prepare CI analyses as requested by the DUSD(P).

i. Establish and maintain liaison with FCI and security agencies in accordance with policies formulated by the Director of Central Intelligence and as provided in E.O. 12333 (reference (b)) and coordinate Military Department programs and activities with other U.S. Government organizations.

j. Participate on DoD, national, international, and interdepartmental boards, committees, and other organizations involving CI as requested by the DUSD(P).

3. The *Director, Defense Intelligence Agency,* shall:

a. Prepare joint and DoD-level multidisciplinary analyses of foreign intelligence and international terrorist threats to joint and DoD-level military security interests.

b. Coordinate the CI production programs of the Military Departments and publish annually a DoD CI production schedule and a DoD CI Publications Registry.

c. Ensure that adequate, timely, and reliable CI analysis and production support is provided to the JCS and the Unified and Specified Commands.

d. Establish and maintain a DoD CI data base, consistent with DoD Directive 5000.19 (reference (e)), to support the DoD CI production efforts of the DoD Components concerned.

e. Participate on DoD, national, international, and interdepartmental boards, committees, and other organizations involving CI as requested by the DUSD(P).

f. Provide staff support to the Chairman, JCS, on NSC matters and represent the interests of the Chairman, JCS, on the DCIB.

4. The *Director, National Security Agency/Chief, Central Security Service,* shall:

a. Collect, process, and disseminate signals intelligence information for CI purposes.

b. Participate in the production of multidisciplinary intelligence threat analyses as required.

c. Participate on DoD, national, and interdepartmental boards, committees, and other organizations involving CI as requested by the DUSD(P).

5. The *Heads of DoD Components (except Military Department Secretaries)*

a. Refer matters of a CI nature involving:

(1) Military personnel assigned to their Components to the Military Department concerned for appropriate investigation and disposition.

(2) Civilian personnel employed by their Components in the United States to the Federal Bureau of Investigation (FBI) and, when overseas, to the Military Department responsible for providing administrative and logistical support.

b. Request the Military Departments, DIA, and NSA/CSS to provide CI support and information, as provided in subsections H.2. through H.4., above.

c. Notify the DUSD(P) when such referrals or requests are made and a Military Department, Defense Agency, or the FBI declines to provide requested CI support or information.

I. Effective Date and Implementation

This Directive is effective immediately. Existing implementing documents still are adequate; no further implementation is necessary.

Signed by PAUL THAYER
Deputy Secretary of Defense

Appendix C
Extract from "The Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979"

Section 6
Delineation of responsibility for CI investigations

Responsibility for CI investigations shall be apportioned between the FBI and the military CI services of the DOD as follows:

a. All investigations of violations of the Atomic Energy Act of 1946, which might constitute a CI investigation as defined herein, shall be the responsibility of the FBI, regardless of the status or location of the subjects of such investigations.

b. Except as provided by paragraph c(2) herein, all CI investigations of foreign nationals undertaken within the United States shall be the responsibility of the FBI.

c. CI investigations within the United States shall be conducted in accordance with the following jurisdictional guidelines:

(1) Except as provided herein, investigations of all civilians, including DOD civilian personnel, shall be the responsibility of the FBI;

(2) Investigations of US military personnel on active duty shall be the responsibility of the CI service of the appropriate military department;

(3) Investigations of retired military personnel, active and inactive reservists, and National Guard members shall be the responsibility of the FBI; provided, however, that investigations of actions which took place while the subject of the investigation was, or is, on active military duty shall be conducted by the CI service of the appropriate military department; and,

(4) Investigations of private contractors of the DOD, and their employees, shall be the responsibility of the FBI, *Provided*, however, that nothing contained in this paragraph shall prevent the military CI services of the DOD, in a manner consistent with applicable law and Executive Branch policy, from undertaking:

(a) In those cases where the FBI chooses to waive investigative jurisdiction, investigative actions which are necessary to establish or refute the factual basis required for an authorized administrative action, to protect the security of its personnel, information, activities, and installations; or

(b) To provide assistance to the FBI in support of any CI investigation for which the FBI is herein assigned responsibility.

d. CI investigations outside the United States shall be conducted in accordance with the following guidelines:

(1) Investigations of military personnel on active duty shall be the responsibility of the military CI services of the DOD.

(2) Investigations of current civilian employees, their dependents, and the civilian dependents of active duty military personnel shall be the responsibility of the military CI services, unless such responsibility is otherwise assigned pursuant to agreement with the host government, US law or Executive directive.

(3) Investigations of retired military personnel, active and inactive reservists, National Guard members, private contractors and their employees, and other US persons, who permanently reside in such locations, shall be undertaken in consultation with the FBI, CIA, and host government as appropriate, *Provided*, however, that nothing contained in this paragraph shall prevent the military CI services of the DOD, in a manner consistent with applicable law and Executive Branch policy from undertaking:

(a) Investigative actions which are necessary to establish or refute the factual basis required for an authorized administrative action, to protect the security of its personnel, information, activities, and installations; or

(b) To provide assistance to the FBI or security service of a host government in support of CI investigations outside the United States for which DOD is not herein assigned investigative responsibility.

(Appropriate letterhead)

(Office symbol) *(date)*

SUBJECT: Lost or Stolen U.S. Army Intelligence Badge

(Name and address of agency to which loss is being reported)

1. It is requested that the following information be disseminated to the appropriate offices of your organization:

a. U.S. Army Intelligence badge number *(badge number)* issued to special agent *(name of agent)*, has been lost or stolen on or about *(date of loss)* in the vicinity of *(place of loss)*.

b. The badge is 2-by 1 1/2-inches in size, made of a gold-colored alloy in the shape of a shield surmounted by the figure of an eagle. On the top of the shield proper, in blue lettering, are the words "Department of the Army." On the bottom of the shield are the words "Military Intelligence," also in blue lettering. In the center of the shield between the two legends is an engraved seal with the legend "United States of America War Office" around its rim. On either side of the engraved insignia in the center are letters "U" and "S" in large capitals. The badge is stamped on the reverse with a number.

2. If the above badge is found or any information is obtained that may lead to its recovery, please forward it to *(complete address where badge is to be sent)*.

(Signature of notifying official)

Figure 9–1. Sample notification letter for lost or stolen badge

(Appropriate letterhead)

(Office symbol) *(date)*

SUBJECT: Lost or Stolen U.S. Army Intelligence Credentials

(Name and address of agency to which loss is being reported)

1. U.S. Army Intelligence credentials number *(credentials number)* issued to special agent *(name of agent)*, has been lost or stolen on or about *(date of loss)* in the vicinity of *(place of loss)*.

2. The U.S. Army Intelligence credentials are encased in a leather wallet-type holder, approximately 3 1/2- by 5-inches in size. The credentials consist of two laminated parts, approximately 3- by 4 1/2-inches in size. Each portion bears the U.S. Army watermark. The upper laminated portion is identified by the name of the special agent that appears printed within the certification statement. The credentials number is centered below the certification statement. The lower laminated portion of the credentials is identified by the official mission certification in the upper left corner and a color photograph of the special agent in the upper right corner. The official signature block of the Chief of Staff, U.S. Army, appears in the center of the credentials. In addition, this portion of the credentials contains the signature of The Adjutant General, U.S. Army, and the signature of the special agent to whom it was issued. The credentials number is printed below the signature of the special agent.

3. If the above credentials are found or any information is obtained that may lead to their recovery, please forward to *(complete address to where credentials/information are to be sent)*.

(Signature of notifying official)

Figure 9–2. Sample notification letter for lost or stolen credentials

Glossary

Section I
Abbreviations

ACSI
Assistant Chief of Staff for Intelligence

ADPSSEP
Automated Data Processing Systems Security Enhancement Program

AOC
Army Operations Center

AOR
area of responsibility

ARNG
Army National Guard

CI
counterintelligence

CIA
Central Intelligence Agency

CID
Criminal Investigation Division

CINCUSAREUR
Commander-in-Chief, U.S. Army Europe

COMSEC
communications security

DA
Department of the Army

DCSOPS
Deputy Chief of Staff for Operations and Plans

DIA
Defense Intelligence Agency

DOD
Department of Defense

EAC
echelons above corps

ECB
echelons corps and below

ECCM
electronic counter-countermeasures

ELSEC
electronic security

EW
electronic warfare

FBI
Federal Bureau of Investigation

FI
foreign intelligence

GC
General Counsel

HQDA
Headquarters, Department of the Army

HUMINT
human intelligence

IIR
Intelligence Information Report

IMINT
imagery intelligence

INSCOM
U.S. Army Intelligence and Security Command

KAWOL
knowledgeable person absent without leave

MACOM
major Army command

MED
manipulative electronic deception

MI
military intelligence

MICECP
Military Intelligence Civilian Excepted Career Program

MILPERCEN
U.S. Army Military Personnel Center

MOS
military occupational specialty

OACSI
Office of the Assistant Chief of Staff for Intelligence

OPSEC
operations security

OSE
Operations Security Evaluation

OSS
operations security services

PMO
provost marshal's office

PSA
Project Security Analysis

RNA
rations not available

SAEDA
subversion and espionage directed against U.S. Army

SAP
special access program

SIGINT
signals intelligence

SIGSEC
signals security

SSI
specialty skills identifier

SSN
Social Security Number

TAREX
target exploitation

TDY
temporary duty

TSCM
technical surveillance countermeasures

USACIDC
U.S. Army Criminal Investigation Command

USAIA
U.S. Army Intelligence Agency

USAICS
U.S. Army Intelligence Center and School

USAITAC
U.S. Army Intelligence and Threat Analysis Center

USAR
U.S. Army Reserve

USAREUR
U.S. Army Europe

Section II
Terms

Army civilian personnel
Includes all U.S. citizen officers and employees of the Army not on active military duty, and all foreign nationals employed by the Army.

Assassination
The murder or attempted murder of Army personnel or employees for political or retaliatory reasons by terrorists or agents of a foreign power.

Compromising emanations
Unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose national security information transmitted, received, handled, or otherwise processed by any information processing system. Often referred to by the short name "TEMPEST."

Counterintelligence
Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations, conducted for or on behalf of foreign powers, organizations or persons, or terrorist activities, but not including personnel,

physical, document, or communications security programs.

Counterintelligence collection

The acquisition of information of a counterintelligence nature by means of direct observation, liaison with official agencies, or solicitation from other sources in response to officially approved counterintelligence collection requirements. Counterintelligence collection may be developed during investigations or operations, or may be acquired for the specific purpose of satisfying a requirement. Information will be considered as "collected" only when it has been made part of the files or information holdings of an Army intelligence component.

Counterintelligence investigation

The systematic collection of information regarding a person or group, which is or may have engaged in espionage or other clandestine intelligence activity, sabotage, terrorist activities, or assassinations, conducted for, or on behalf of, foreign powers, organizations, or persons.

Counterintelligence operations

Actions taken against hostile intelligence services to counter espionage and other clandestine intelligence activities damaging to national security.

Counterintelligence production

The process of converting significant counterintelligence information into intelligence through the evaluation, analysis, integration and interpretation of all source data.

Defector

A person who unlawfully and voluntarily leaves U.S. control and allows himself/herself to come under the control of a foreign power with interests inimical to those of the United States.

Deliberate compromise

The act, attempt, or reported contemplation by Army personnel of intentionally conveying classified documents, information, or material to any unauthorized person, to include public disclosure in an unauthorized manner.

Detainee

A person who inadvertently or involuntarily comes under the control of a nation or hostile force with interests inimical to those of the United States.

Espionage

The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The elements of espionage are set forth in 18 USC 792-798.

Knowledgeable AWOL

A military individual absent without leave and designated by a major commander as having knowledge of, and recent access to, national defense information classified Secret or higher, or COMSEC information, the unauthorized disclosure of which would result in serious damage or exceptionally grave danger to the United States.

Multidiscipline CI Analysis

Work involving the assessments of threats to U.S. security presented by activities of hostile intelligence collection systems. Includes all-source analysis of the integrated, combined effort of hostile collection disciplines, and SIGINT, HUMINT, and IMINT, and special operations controlled by hostile intelligence agencies.

Operations Security Evaluation (OSE)

A specialized, integrated, multidisciplinary analysis of military operations and activities to identify weaknesses that could compromise current or future plans or operations.

Project Security Analysis (PSA)

An OSE that is conducted for a specific activity within a larger organization.

Sedition

Participation in one or more of the following:

a. Knowingly or willfully advocating or teaching the duty or necessity of overthrowing the United States Government or any political subdivision therein by force or violence.

b. Printing, publishing, circulating, selling or publicly displaying written matter, with intent to cause the overthrow or destruction of any such government, which advocates or teaches the duty or necessity of such overthrow by force or violence.

c. Organizing a society or group whose purpose is to advocate or teach the duty or necessity of such overthrow by force or violence.

d. Being or becoming a member of, or affiliated with, such society or group knowing the purpose thereof.

Subversion

Includes the following:

a. Actively encouraging military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities;

b. With the willful intent thereby to interfere with, or impair the loyalty, morale or discipline of the military forces of the United States.

TEMPEST

A short name referring to investigations and studies of compromising emanations. It is often used synonymously for the term compromising emanations.

Terrorist activities

The actual commission of violent acts, threat of violent acts to attain goals poli cal, religious, or ideological in nature. Th is done through intimidation, coercion, instilling fear. Terrorist activities are crin nal acts that are often symbolic in natu and intended to influence an audience b yond its immediate victims.

Terrorism counteraction

Defensive measures (antiterrorism) to r duce the vulnerability to terrorist activiti and offensive measures (counterterrorism taken in response to terrorist activities.

RESERVED

U.S. ARMY INTELLIGENCE BADGE AND CREDENTIALS RECEIPT AND/OR TRACER

For use of this form, see AR 381-20; the proponent agency is OACSI.

ADDRESSEE	*RETURN THIS RECEIPT TO ADDRESS ON REVERSE* DATE DISPATCHED OR ISSUED REGISTER OR CONTROL NUMBER

☐ BADGE _____ (Number) ☐ CREDENTIALS _____ (Number) ☐ BADGE AND CREDENTIALS _____ (Number)

☐ DISPATCHED ☐ ISSUED	☐ SURRENDERED TO CUSTODIAN/SUBCUSTODIAN SIGNATURE OF CUSTODIAN/SUBCUSTODIAN	DATE

☐ TRACER ACTION DESIRED - SIGNED COPY OF RECEIPT FOR MATERIAL DESCRIBED ABOVE HAS NOT BEEN RECEIVED.
(PLEASE ACCOMPLISH APPROPRIATE SPACES BELOW AND RETURN AT ONCE)

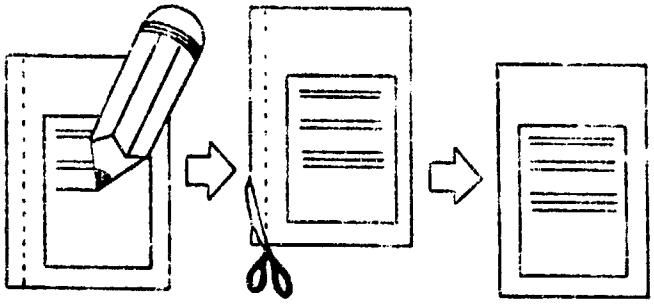
☐ RECEIPT OF ITEM(S) ACKNOWLEDGED ☐ ITEM(S) HAVE NOT BEEN RECEIVED

DATE	TYPED NAME, GRADE OR TITLE	SIGNATURE

DA FORM 1 AUG 75 4354-R

* U.S. GOVERNMENT PRINTING OFFICE: 1986- 490-999:4035

ARMY UPDATE PUBLICATIONS SUBSCRIPTION FORM



Fill out... Detach...

Forward to unit publications officer for consolidation on DA Form 12-9U-R.

This page is for internal use within your unit.

1. To change their initial distribution requirements, individual users or sections of a unit should complete this DA Form 12-13 (UPDATE Subscription Page) and submit it to their unit publications officer.

2. The unit publications officer should consolidate the entire unit's requirements, enter those requirements on DA Form 12-9U-R, and submit the DA 12-9U-R to the address preprinted on the form. Only unit publications officers may submit DA Form 12-9U-R (DA 12-Series Circular)

(Publication No AR 381-20

To: Publications Officer

FOR COMPLETION BY USER OF PUBLICATION

From: (Organization, Name, and Telephone Number)

Number of copies desired for section use

Current number of copies received

DA FORM 12-13, Previous editions of DA Form 12-13 are obsolete and may not be used